

TRANSMITTAL OF INFORMATION DISCLOSURE STATEMENT
(Under 37 CFR 1.97(b) or 1.97(c))

Docket No.
T00001-0378-US1

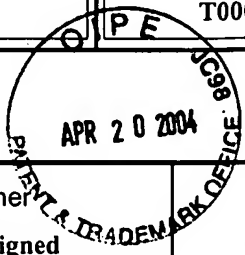
In Re Application Of: **VANSTONE, Scott A. et al.**

Serial No.
10/765,976

Filing Date
January 29, 2004

Examiner
Not Yet Assigned

Group Art Unit
Not Yet Assigned



Title: **DIGITAL SIGNATURES ON A SMARTCARD**

Address to:
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

37 CFR 1.97(b)

1. ☒ The Information Disclosure Statement submitted herewith is being filed within three months of the filing of a national application other than a continued prosecution application under 37 CFR 1.53(d); within three months of the date of entry of the national stage as set forth in 37 CFR 1.491 in an international application; before the mailing of a first Office Action on the merits, or before the mailing of a first Office Action after the filing of a request for continued examination under 37 CFR 1.114.

37 CFR 1.97(c)

2. ☐ The Information Disclosure Statement submitted herewith is being filed after the period specified in 37 CFR 1.97(b), provided that the Information Disclosure Statement is filed before the mailing date of a Final Action under 37 CFR 1.113, a Notice of Allowance under 37 CFR 1.311, or an Action that otherwise closes prosecution in the application, and is accompanied by one of:

☐ the statement specified in 37 CFR 1.97(e);

OR

☐ the fee set forth in 37 CFR 1.17(p).

TRANSMITTAL OF INFORMATION DISCLOSURE STATEMENT
(Under 37 CFR 1.97(b) or 1.97(c))

Docket No.
T00001-0378-US1

In Re Application: VANSTONE, Scott A. et al.

Serial No.
10/765,976

Filing Date
January 29, 2004

Examiner
Not Yet Assigned

Group Art Unit
Not Yet Assigned

DIGITAL SIGNATURES ON A SMARTCARD

Payment of Fee

(Only complete if Applicant elects to pay the fee set forth in 37 CFR 1.17(p))

- ☐ A check in the amount of _____ is attached.
- ☐ The Director is hereby authorized to charge and credit Deposit Account No. _____ as described below.
- ☐ Charge the amount of _____
- ☐ Credit any overpayment.
- ☐ Charge any additional fee required.

Certificate of Transmission by Facsimile*

I certify that this document and authorization to charge deposit account is being facsimile transmitted to the United States Patent and Trademark Office (F:

(Date)

Signature

Typed or Printed Name of Person Signing Certificate

Certificate of Mailing by First Class Mail

I certify that this document and fee is being deposited on _____ with the U.S. Postal Service as first class mail under 37 C.F.R. 1.8 and is addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Signature of Person Mailing Correspondence

Typed or Printed Name of Person Mailing Certificate

*This certificate may only be used if paying by deposit account.

Dated: 16 April

Signature
John R.S. Orange (Reg. 29,725)
McCarthy Tetrault LLP
Suite 4700, Box 48
66 Wellington Street West
Toronto Dominion Bank Tower
Toronto, Ontario
M5K 1E6 Canada

CC:



ATTORNEY DOCKET NO.: T00001-0378-US1
CUSTOMER NUMBER: 000027155

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

In re patent application of:

VANSTONE

Serial No.: 10/765,976 Group Art Unit: NOT YET SPECIFIED
Filed: January 29, 2004 Examiner: NOT YET SPECIFIED
Title: **DIGITAL SIGNATURES ON A SMARTCARD**

Mail Stop DD
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

INFORMATION DISCLOSURE STATEMENT

Pursuant to the duty to disclose under 37 CFR §1.56, Applicant submits herewith a Form PTO/SB/08A listing references of which the Applicant is aware and which are brought to the attention of the Examiner. In accordance with 37 CFR §1.98(a)(2), a copy of each document listed in the enclosed Form PTO/SB/08A-8B is submitted herewith excluding U.S. patent references.

U.S. patent references are not enclosed pursuant to the Office's waiver (published in the Official Gazette - August 5, 2003) of such requirement for all U.S. national patent applications and for all international applications that have entered the national stage under 35 USC 371 filed after June 30, 2003.

Pursuant to 35 USC §120, this application relies on the earlier filing date(s) of the following prior application(s):

<u>Serial Number</u>	<u>Filing Date</u>
09/942,492	August 29, 2001
09/434,247	November 5, 1999
08/632,845	April 16, 1996

The filing of this IDS shall not be construed as a representation that a search has been made, an admission that the information cited is, or is considered to be, material for patentability, or that no other material information exists. This filing shall not be construed as an admission against interest in any matter.

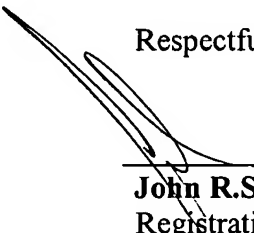
This IDS is submitted pursuant to 37 CFR §1.97(b) and, accordingly, no fee is believed to be due for consideration of the documents submitted herewith.

Applicant respectfully requests consideration of the items listed and requests the Examiner to return a copy of the attached Form PTO/SB/08A-8B after being marked as being considered by the Examiner.

Date:

16 April 04

Respectfully submitted,



John R.S. Orange
Registration No. 29,725
Agent for Applicant

McCarthy Tétrault
Suite 4700, P.O. Box 48
Toronto Dominion Bank Tower
Toronto, Ontario M5K 1E6, Canada

Tel: 416 362-1812
Fax: 416 601-8454

Complete if Known

Application Number	10/765,976
Filing Date	January 29, 2004
First Named Inventor	VANSTONE
Art Unit	NOT YET SPECIFIED
Examiner Name	NOT YET SPECIFIED
Attorney Docket Number	T00001-0378-US1

(use as many sheets as necessary)

Sheet	1	of	2	Attorney Docket Number	T00001-0378-US1
-------	---	----	---	------------------------	-----------------

[illegible][illegible]

Date Considered

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449B/PTO

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**

(use as many sheets as necessary)

Sheet 2 of 2

Complete if Known

Application Number	10/765,976
Filing Date	January 29, 2004
First Named Inventor	VANSTONE
Art Unit	NOT YET SPECIFIED
Examiner Name	NOT YET SPECIFIED
Attorney Docket Number	T00001-0378-US1

OTHER PRIOR ART -- NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ²
		KOBLITZ, "CM-Curves with Good Cryptographic Properties", Advances in Cryptology. Santa Barbara, Aug. 11-15, 1991, Proceedings of the Conference on Theory and Applications of Cryptographic Techniques, Berlin, Springer, DE, 1991, pages 279-287.	
		MEIER W ET AL, "Efficient Multiplication on Certain Nonsupersingular Elliptic Curves", Advances in Cryptology. Santa Barbara, Aug. 16-20, 1992, Proceedings of the Annual International Cryptology Conference, Berlin, Springer, DE, vol. CONF. 12, pages 333-344.	
		SCHOOF R, "Elliptic Curves over Finite Fields and the Computation of Square Roots Mod P", Mathematics of Computation, American Mathematical Society, US, vol. 44, no. 169/170, April 1985, pages 483-494.	
		LAY G-J ET AL, "Constructing Elliptic Curves with Given Group Order Over Large Finite Fields", Algorithmic Number Theory, International Symposium, 1994, pages 250-263.	
		MUELLER V, "Fast Multiplication on Elliptic Curves over Small Fields of Characteristic Two", PUBLICATIONS, TU DARMSTADT, 1997	
		SCHNEIER, "Applied Cryptography: Protocols, Algorithms, and Source Code in C", 1994, pages 39-41, John Wiley & Sons, New York.	

Examiner Signature	Date Considered
--------------------	-----------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not

¹ Applicant's unique citation designation number (optional). ² Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 120 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.